

CLAIMS

What is claimed is:

- 1 1. A descrambler comprising:
 - 2 a non-volatile memory to store a unique key;
 - 3 a control word key ladder logic to produce (i) a
 - 4 first value generated based on a conditional access (CA)
 - 5 random value and the unique key, (ii) a second value
 - 6 generated using the first value, and (iii) a third value
 - 7 recovered using the second value;
 - 8 a first cryptographic unit to descramble incoming
 - 9 content in a scrambled format based on the third value;
 - 10 and
 - 11 a second cryptographic unit to decrypt incoming
 - 12 encrypted data using the first value.
- 1 2. The descrambler of claim 1 being a single
- 2 integrated circuit.
- 1 3. The descrambler of claim 1 implemented within a
- 2 set-top box.
- 1 4. The descrambler of claim 1, wherein the first
- 2 value is a derivative key generated by performing a
- 3 decryption operation on the CA random value using the
- 4 unique key.
- 1 5. The descrambler of claim 1, wherein the first
- 2 value is a derivative key derived by performing a
- 3 decryption operation on a combination of the CA random
- 4 value and padding data, the combination being at least
- 5 128-bits in length.

1 6. The descrambler of claim 4, wherein the second
2 value is a mating key recovered by performing a decryption
3 operation on a mating key generator using the derivative
4 key, the mating key generator being a message comprising
5 one or more of the following: a manufacturer identifier,
6 a service provider identifier, a conditional access (CA)
7 provider identifier and a mating key sequence number.

1 7. The descrambler of claim 5, wherein the second
2 value is a mating key recovered by performing a decryption
3 operation on at least 128-bits of data comprising a mating
4 key generator being a message comprising one or more of
5 the following: a manufacturer identifier, a service
6 provider identifier, a conditional access (CA) provider
7 identifier and a mating key sequence number.

1 8. The descrambler of claim 6, wherein the third
2 value is a control word recovered by performing a
3 decryption operation on an encrypted control word using
4 the mating key.

1 9. The descrambler of claim 7, wherein the third
2 value is a control word recovered by performing (i) a
3 first decryption operation using the mating key on a first
4 combination of a first encrypted control word and a second
5 encrypted control word, and (ii) a second decryption
6 operation using the mating key on a second combination of
7 a third encrypted control word and a plurality of bits
8 operating as padding for the second combination to be at
9 least 128-bits in length.

1 10. The descrambler of claim 1 further comprising a
2 third cryptographic unit to encrypt the descrambled
3 incoming content prior to transmission to a digital
4 device.

1 11. The descrambler of claim 10 further comprising a
2 copy protection ladder logic to produce a copy protection
3 key used by the third cryptographic unit to encrypt the
4 descrambled incoming content.

1 12. The descrambler of claim 11, wherein the copy
2 protection ladder logic to produce a copy protection key
3 by performing a decryption operation on a concatenation of
4 a random value and a plurality of bits to produce a result
5 being at least 128-bits in length, using a logical
6 derivation being a result of an Exclusive OR (XOR)
7 operation of the unique key and a predetermined value.

1 13. A descrambler comprising:

2 a control word key ladder logic to produce (i) a
3 first value generated from a cryptographic operation on a
4 first random value using a unique key, (ii) a second value
5 recovered from a mating key generator undergoing a
6 cryptographic operation using the first value, and (iii) a
7 control word recovered by decrypting an encrypted control
8 word using the second value; and

9 a first cryptographic unit to descramble incoming
10 content in a scrambled format using the control word.

1 14. The descrambler of claim 13 being a single
2 integrated circuit.

1 15. The descrambler of claim 13 further comprising a
2 second cryptographic unit to decrypt incoming encrypted
3 program data received out-of-band by a digital device
4 implemented with the descrambler.

1 16. The descrambler of claim 15, wherein the
2 encrypted program data comprises an encrypted entitlement
3 management message that comprises at least two of (i) a
4 smart card identifier, (ii) a length field, (iii) a mating
5 key generator, (iv) at least one key identifier and (v) at
6 least one key associated with the at least one key
7 identifiers.

1 17. The descrambler of claim 16, where the mating
2 key generator of the encrypted entitlement management
3 message being a message comprising one or more of the
4 following: a manufacturer identifier, a service provider
5 identifier, a conditional access (CA) provider identifier
6 and a mating key sequence number.

1 18. The descrambler of claim 13 further comprising a
2 copy protection ladder logic to produce a copy protection
3 key based on a plurality of process blocks, wherein
4 a first process block configured to generate a
5 derivative key based on a second random value and either
6 the unique key or a logical derivation of the unique key,
7 a second process block configured to recover a user
8 key from an encrypted user key using the derivative key,
9 and
10 a third process block configured to generate a copy
11 protection key from a copy protection key generator using
12 the user key.

1 19. The descrambler of claim 18 further comprising a
2 third cryptographic unit to encrypt the descrambled
3 incoming content using the copy protection key prior to
4 transmission to a digital device.

1 20. The descrambler of claim 18 further comprising a
2 one-time programmable, non-volatile memory coupled to the
3 control word key ladder logic and the copy protection
4 ladder logic, the non-volatile memory to store the unique
5 key.

1 21. The descrambler of claim 19 further comprising a
2 memory to store the copy protection key, the memory being
3 coupled to the third cryptographic unit.

1 22. A descrambler comprising:
2 a memory to store a unique key;
3 a control word key ladder logic coupled to the
4 memory, the control word ladder logic comprising
5 a first process block configured to generate a
6 first derivative key of the unique key,
7 a second process block configured to generate a
8 mating key from a mating key generator using the
9 first derivative key, and
10 a third process block configured to recover a
11 control word by decrypting an encrypted control word
12 using the mating key;
13 a first cryptographic unit coupled to the control
14 word key ladder logic, the first cryptographic unit to
15 descramble incoming content in a scrambled format using
16 the control word.

1 23. The descrambler of claim 22 being a single
2 integrated circuit.

1 24. The descrambler of claim 22 further comprising a
2 second cryptographic unit to decrypt incoming encrypted
3 program data received out-of-band by a digital device
4 implemented with the descrambler.

1 25. The descrambler of claim 24, wherein the
2 encrypted program data comprises an encrypted entitlement
3 management message that comprises at least two of (i) a
4 smart card identifier, (ii) a length field, (iii) a mating
5 key generator, (iv) at least one key identifier and (v) at
6 least one key associated with the at least one key
7 identifier.

1 26. The descrambler of claim 22 further comprising a
2 copy protection ladder logic coupled to the first
3 cryptographic unit, the copy protection ladder logic
4 comprising

5 a fourth process block configured to generate a
6 second derivative key based on a random value and the
7 unique key;

8 a fifth process block configured to decrypt an
9 encrypted user key using the second derivative key to
10 recover a user key; and

11 a sixth process block configured to generate a copy
12 protection key from a copy protection key generator using
13 the user key.

1 27. The descrambler of claim 26 further comprising a
2 second cryptographic unit to encrypt the descrambled
3 incoming content using the copy protection key prior to
4 transmission to a digital device.

1 28. A descrambler comprising:

2 a non-volatile memory to store a plurality of unique
3 keys;

4 a control word key ladder logic to produce (i) a
5 plurality of derivative keys generated based on a
6 conditional access (CA) random value and a corresponding
7 plurality of unique keys, (ii) a plurality of mating keys

8 generated using the plurality of derivative keys, and
9 (iii) a plurality of control words recovered using the
10 plurality of mating keys; and
11 a first cryptographic unit to descramble incoming
12 content in a scrambled format based on at least one of the
13 plurality of control words.

1 29. The descrambler of claim 28, wherein the
2 plurality of derivative keys comprising:

3 (i) a first derivative key generated by the CA random
4 value undergoing at least three transformations in
5 succession, wherein a first transformation is performed on
6 the CA random using a first unique key of the plurality of
7 unique keys to produce a first result, a second
8 transformation is performed on the first result using a
9 second unique key of the plurality of unique keys to
10 produce a second result, and a third transformation is
11 performed on the second result using a third unique key of
12 the plurality of unique keys to produce the first
13 derivative key,

14 (ii) a second derivative key is generated by the CA
15 random value and a first predetermined value undergoing a
16 bitwise logical operation to produce a fourth result,
17 followed by the fourth result undergoing at least three
18 transformations in succession, wherein a fourth
19 transformation is performed on the fourth result using the
20 first unique key to produce a fifth result, a fifth
21 transformation is performed on the fifth result using the
22 second unique key to produce a sixth result, and a sixth
23 transformation is performed on the sixth result using the
24 third unique key to produce the second derivative key, and
25 (iii) a third derivative key is generated by the CA
26 random value and a second predetermined value, differing
27 from the first predetermined value, undergoing a bitwise

28 logical operation to produce a seventh result, followed by
29 the seventh result undergoing at least three
30 transformations in succession, wherein a seventh
31 transformation is performed on the seventh result using
32 the first unique key to produce an eighth result, a eighth
33 transformation is performed on the eighth result using the
34 second unique key to produce a ninth result, and a ninth
35 transformation is performed on the ninth result using the
36 third unique key to produce the third derivative key.

1 30. The descrambler of claim 28, wherein the
2 plurality of mating keys comprising
3 (i) a first mating key generated by a mating key
4 generator, being a message that comprises at least one of
5 a manufacturer identifier, a service provider identifier,
6 a conditional access (CA) provider identifier and a mating
7 key sequence number, undergoing at least three
8 transformations in succession, wherein a first
9 transformation being performed on the mating key generator
10 using a first derivative key of the plurality of
11 derivative keys to produce a first result, a second
12 transformation being performed on the first result using a
13 second derivative key of the plurality of derivative keys
14 to produce a second result, and a third transformation
15 being performed on the second result using a third
16 derivative key of the plurality of derivative keys to
17 produce the first mating key,
18 (ii) a second mating key generated by the mating key
19 generator and a first predetermined value undergoing a
20 bitwise logical operation to produce a third result,
21 followed by the third result undergoing at least three
22 transformations in succession, wherein a fourth
23 transformation being performed on the third result using
24 the first derivative key to produce a fourth result, a

25 fifth transformation being performed on the fourth result
26 using the second derivative key to produce a fifth result,
27 and a sixth transformation being performed on the fifth
28 result using the third derivative key to produce the
29 second mating key, and

30 (iii) a third mating key is generated by the mating
31 key generator and a second predetermined value, differing
32 from the first predetermined value, undergoing a bitwise
33 logical operation to produce a sixth result, followed by
34 the sixth result undergoing at least three transformations
35 in succession, wherein a seventh transformation being
36 performed on the sixth result using the first derivative
37 key to produce an seventh result, a eighth transformation
38 being performed on the seventh result using the second
39 derivative key to produce an eighth result, and a ninth
40 transformation being performed on the eighth result using
41 the third derivative key to produce the third mating key.

1 31. The descrambler of claim 28, wherein the
2 plurality of control words comprising

3 (i) a first control word recovered by a first
4 encrypted control word undergoing at least three
5 transformations in succession, wherein a first
6 transformation being performed on a first encrypted
7 control word using the first mating key of the plurality
8 of mating keys to produce a first result, a second
9 transformation being performed on the first result using a
10 second mating key of the plurality of mating keys to
11 produce a second result, and a third transformation being
12 performed on the second result using a third mating key of
13 the plurality of mating keys to produce the first control
14 word,

15 (ii) a second control word recovered from a second
16 encrypted control word and a first predetermined value

17 undergoing a bitwise logical operation to produce a third
18 result, followed by the third result undergoing at least
19 three transformations in succession, wherein a fourth
20 transformation being performed on the third result using
21 the first mating key to produce a fourth result, a fifth
22 transformation being performed on the fourth result using
23 the second mating key to produce a fifth result, and a
24 sixth transformation being performed on the fifth result
25 using the third mating key to produce the second control
26 word, and

27 (iii) a third control word recovered from a third
28 encrypted control word and a second predetermined value,
29 differing from the first predetermined value, undergoing a
30 bitwise logical operation to produce a sixth result,
31 followed by the sixth result undergoing at least three
32 transformations in succession, wherein a seventh
33 transformation being performed on the sixth result using
34 the first mating key to produce an seventh result, a
35 eighth transformation being performed on the seventh
36 result using the second mating key to produce an eighth
37 result, and a ninth transformation being performed on the
38 eighth result using the third mating key to produce the
39 third control word.

1 32. The descrambler of claim 30, wherein the bitwise
2 logical operation is an Exclusive OR operation.